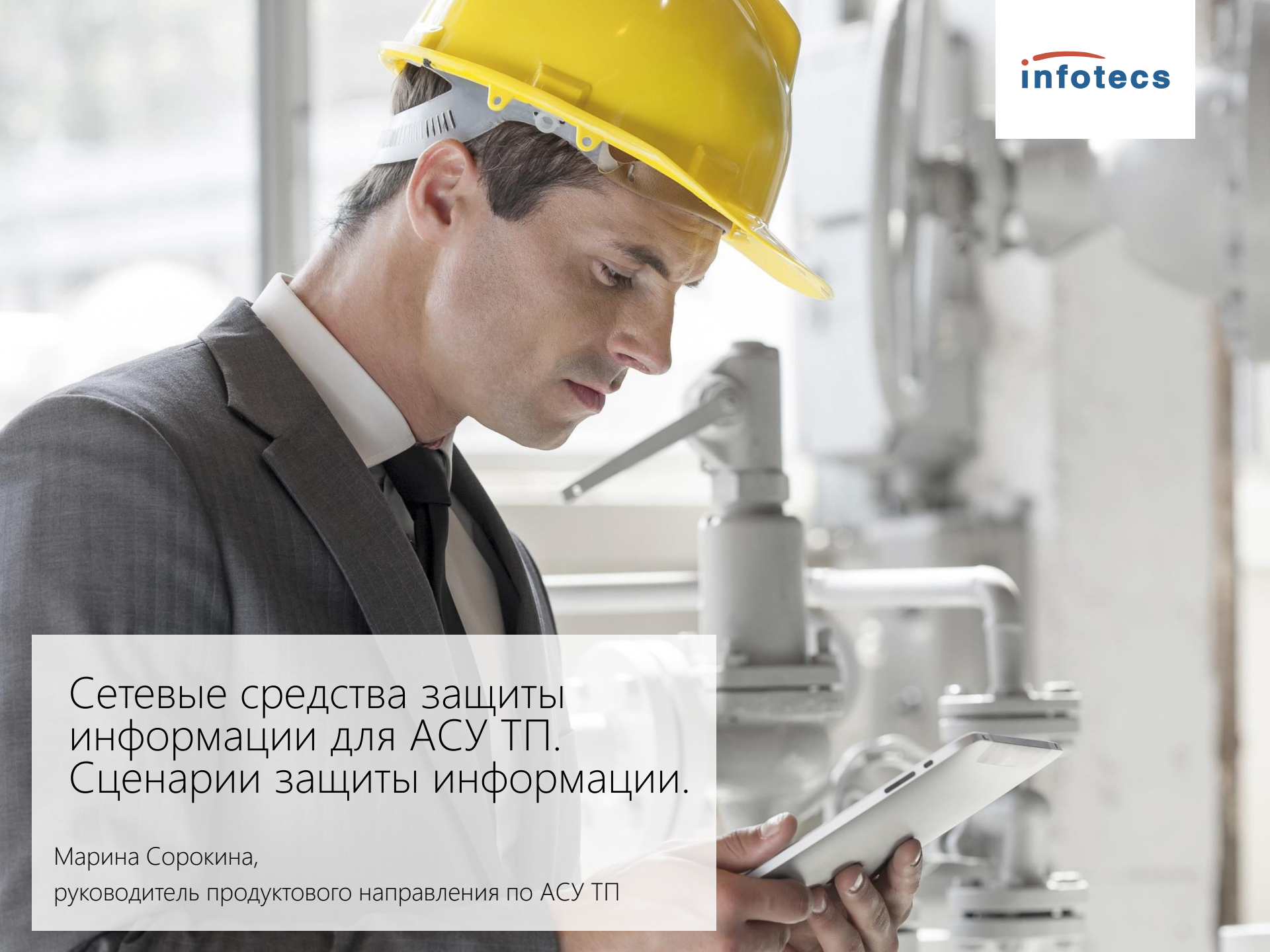


Сетевые средства защиты информации для АСУ ТП. Сценарии защиты информации.

Марина Сорокина,
руководитель продуктового направления по АСУ ТП

Кибератаки

2010

Иран, Stuxnet

Остановка Иранских центрифуг вирусом Stuxnet

2014

Германия, металлургия

Кибератака на сталелитейный завод в Германии

2015

Япония, электроэнергетика

Атака на АЭС в Японии

2015

США, Автомобильная отрасль

Дистанционный взлом Чарли Миллером и Крисом Веласеком Jeep Cherokee

2015

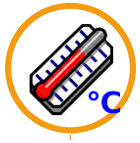
Украина, электроэнергетика

Погашение 7 подстанций 110кВ и 23 подстанции 35кВ на Украине

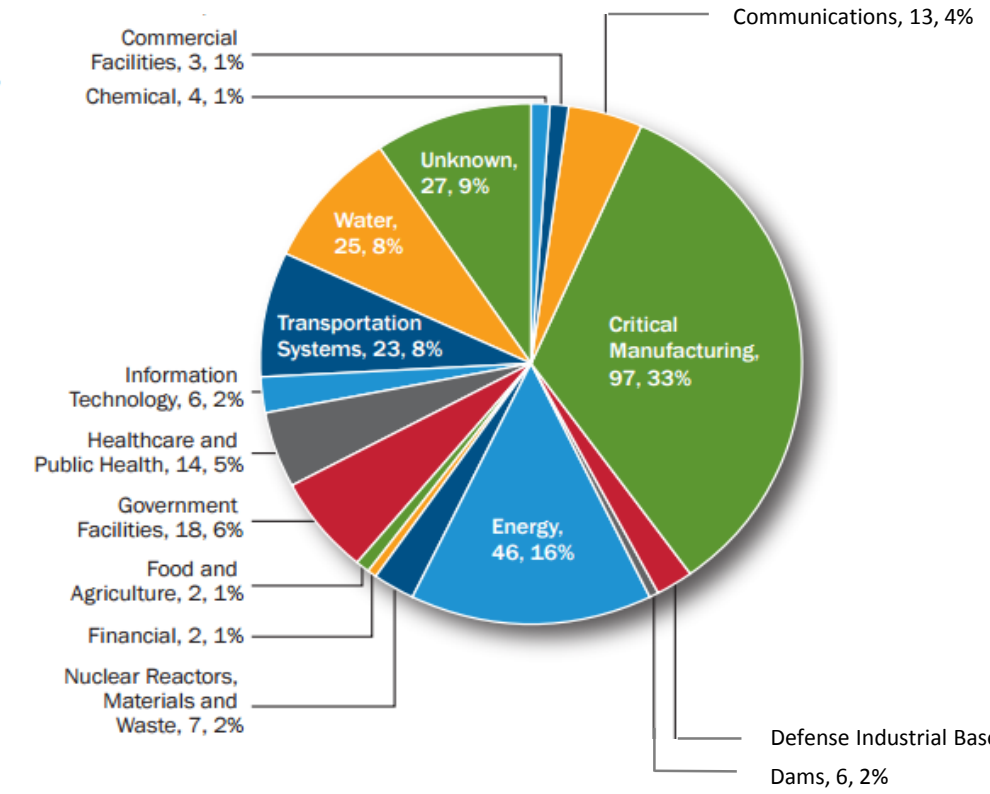
ноябрь 2016

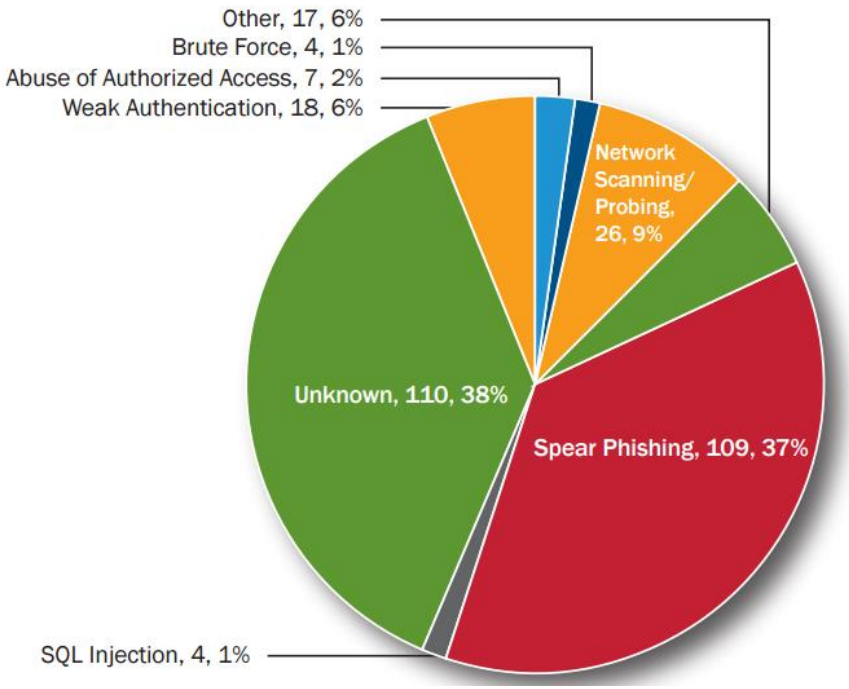
Финляндия, DDos-атака

Несколько многоквартирных домов в финском городе Лаппеэнранта остались без теплоснабжения в результате DDoS-атаки.



Статистика инцидентов АСУ ICS-CERT за 2015 г.

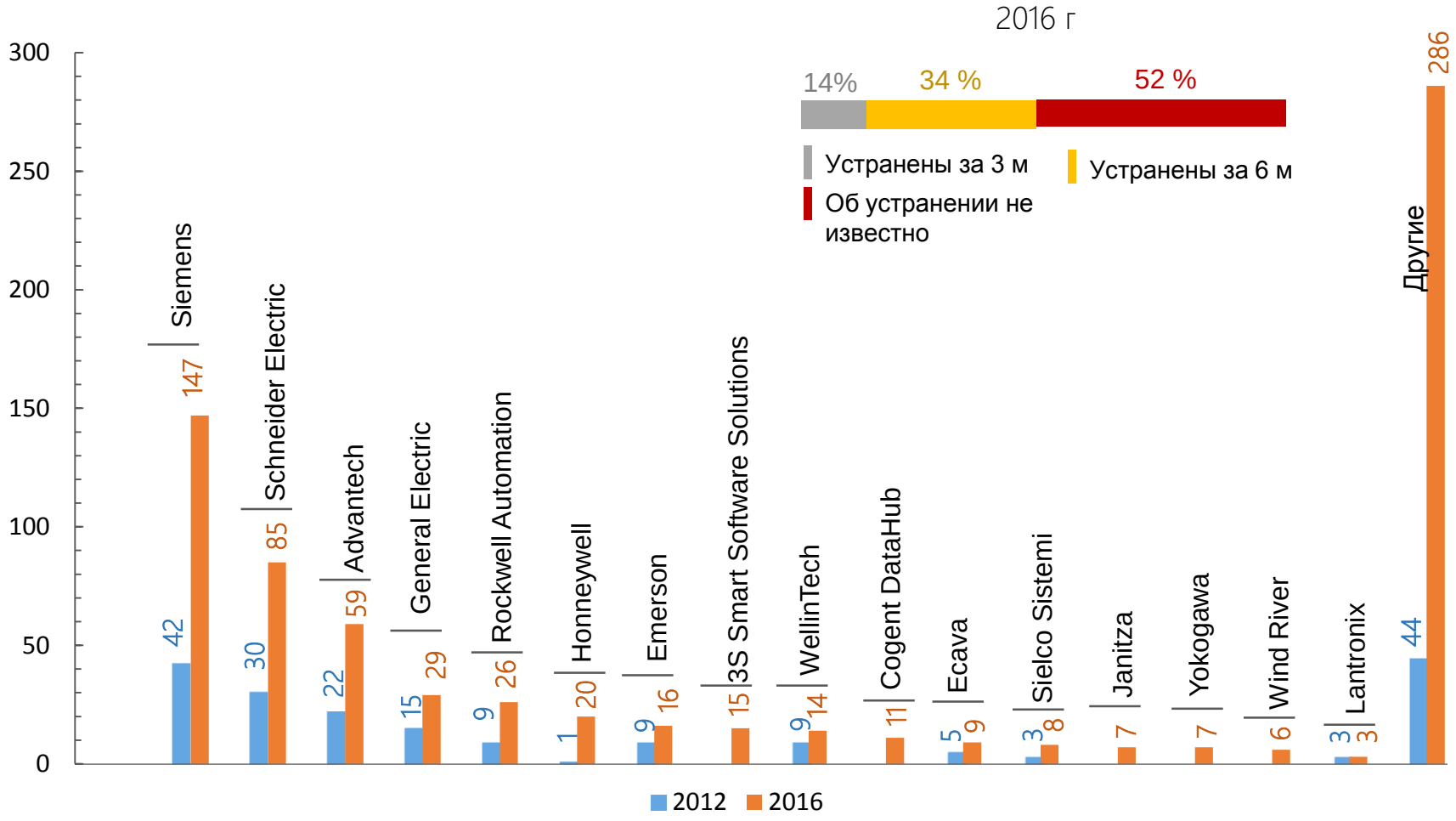




Всего 295 инцидентов, 8 из которых привели к ущербу, превышающему 1 млн.долларов

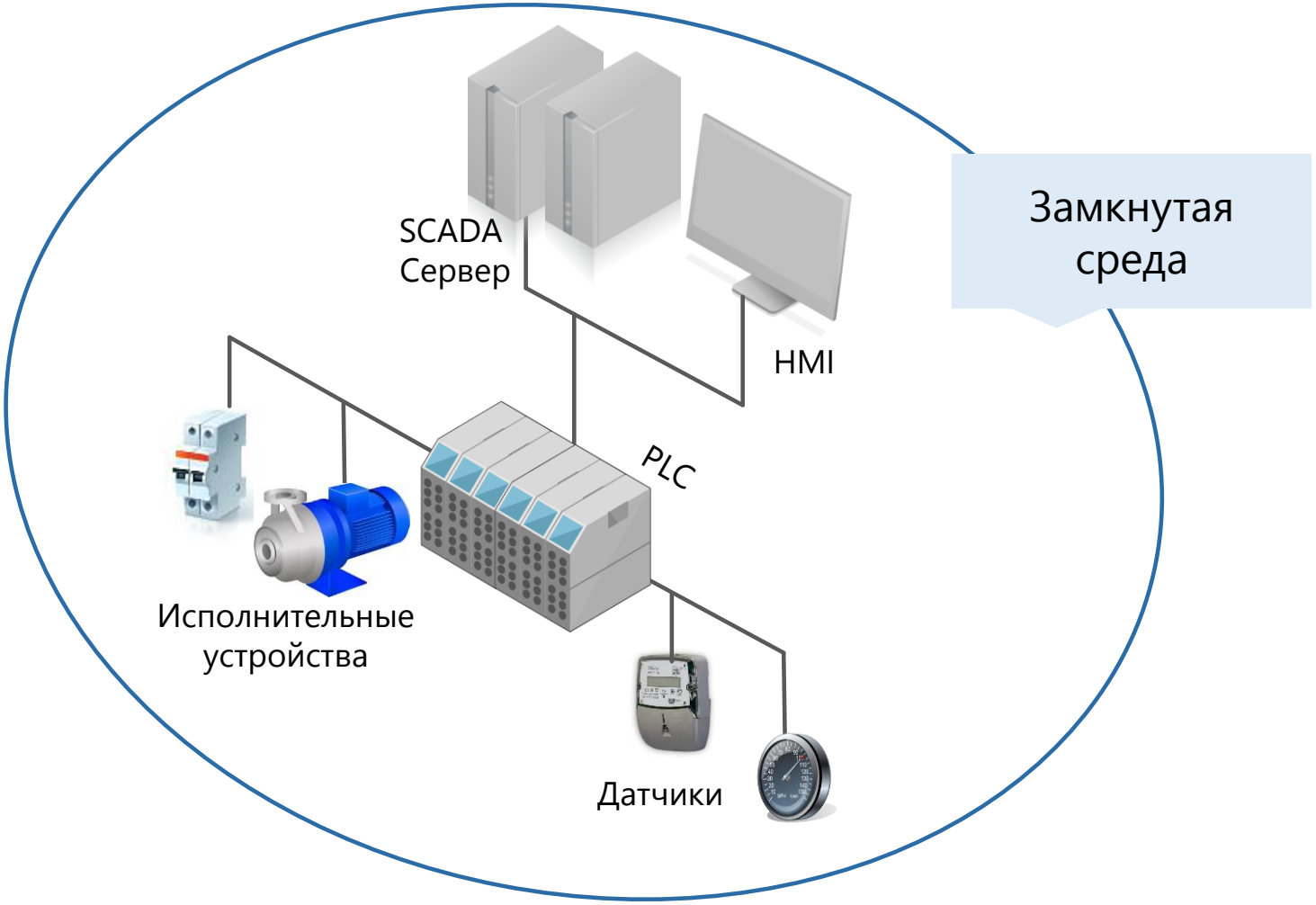
https://ics-cert.us-cert.gov/ics-archive

Количество уязвимостей компонентов АСУ ТП различных производителей

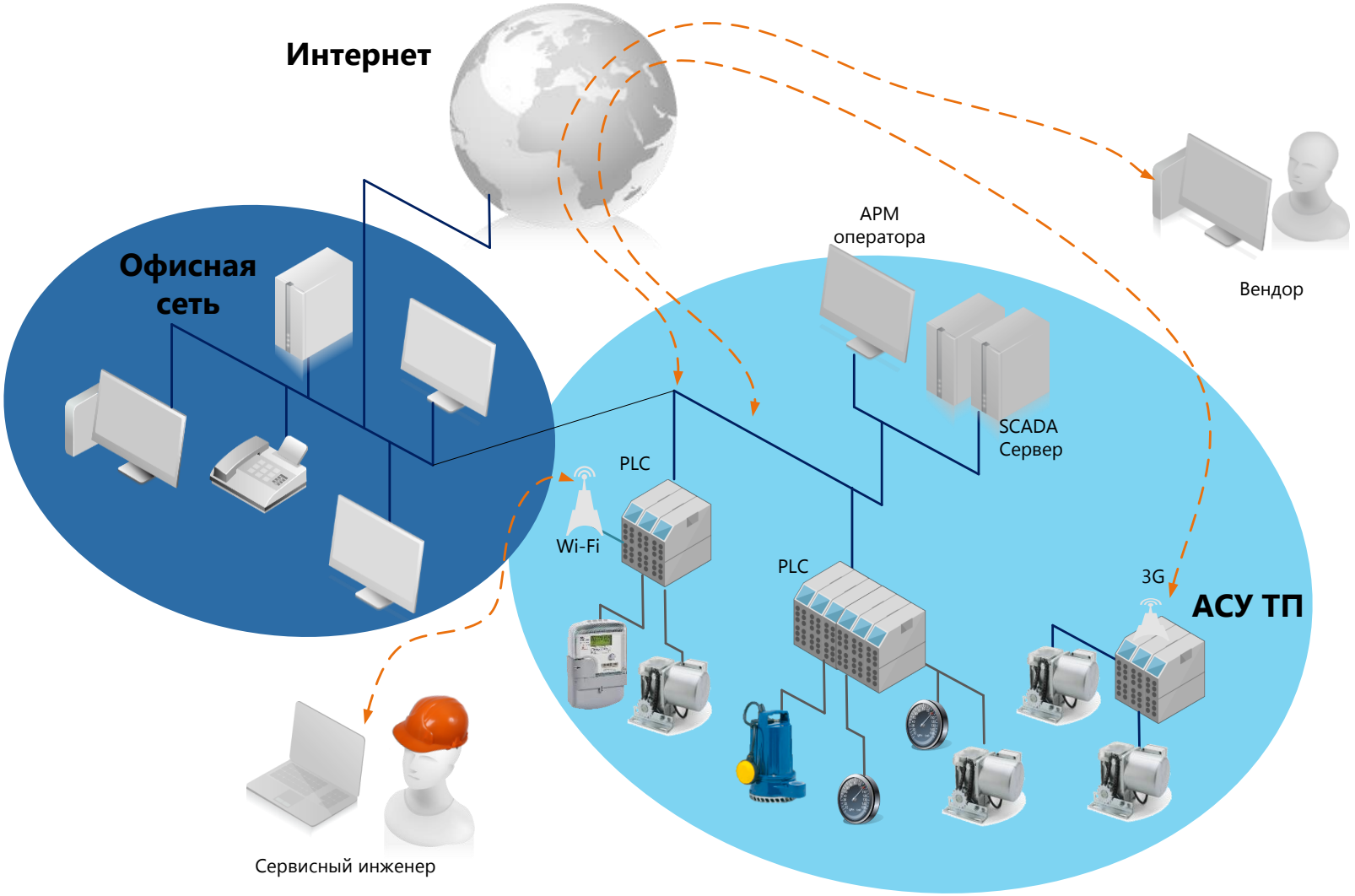


https://www.ptsecurity.com/upload/ptru/analytics/ICS-Vulnerability-2016-rus.pdf

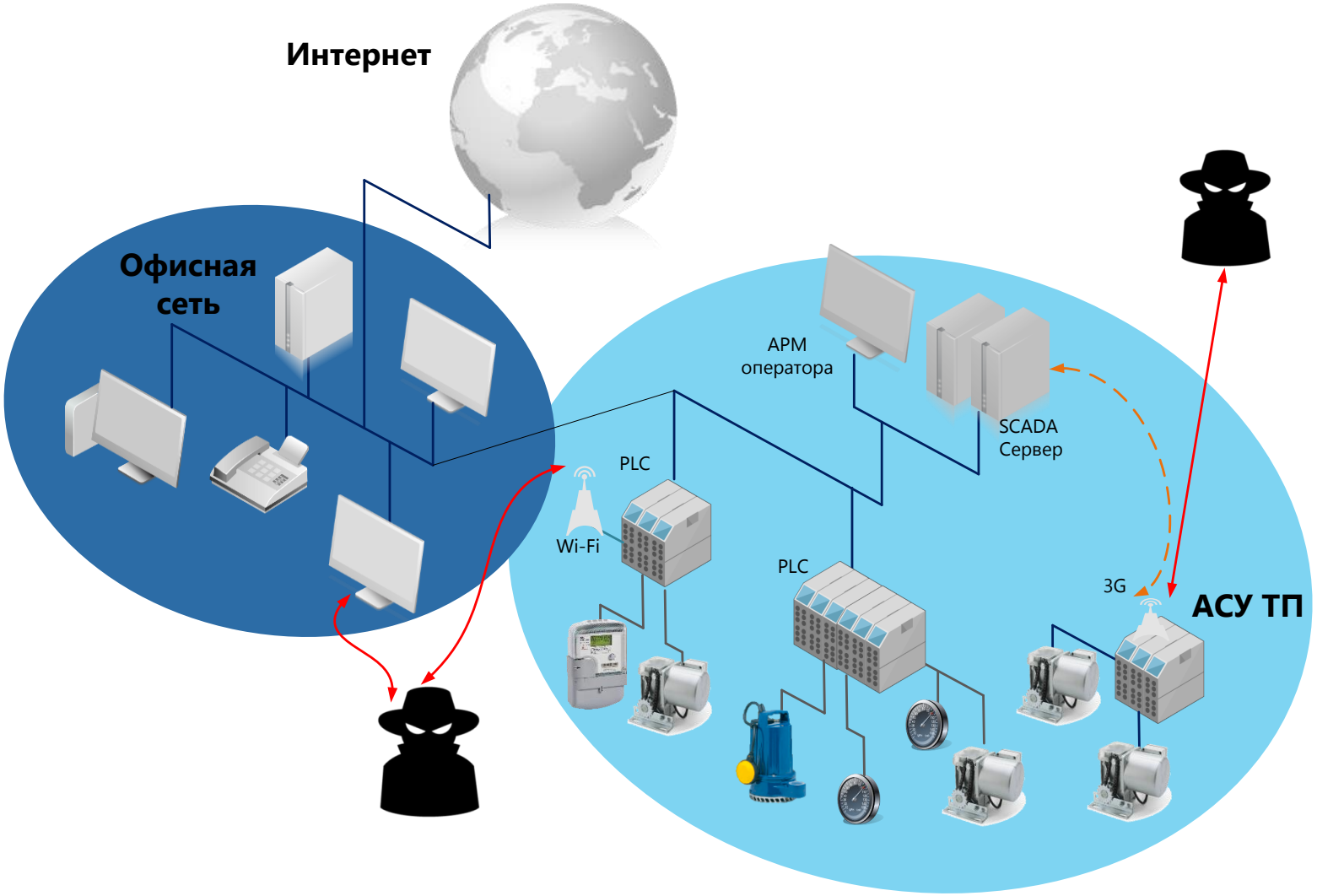
Классическая АСУ ТП



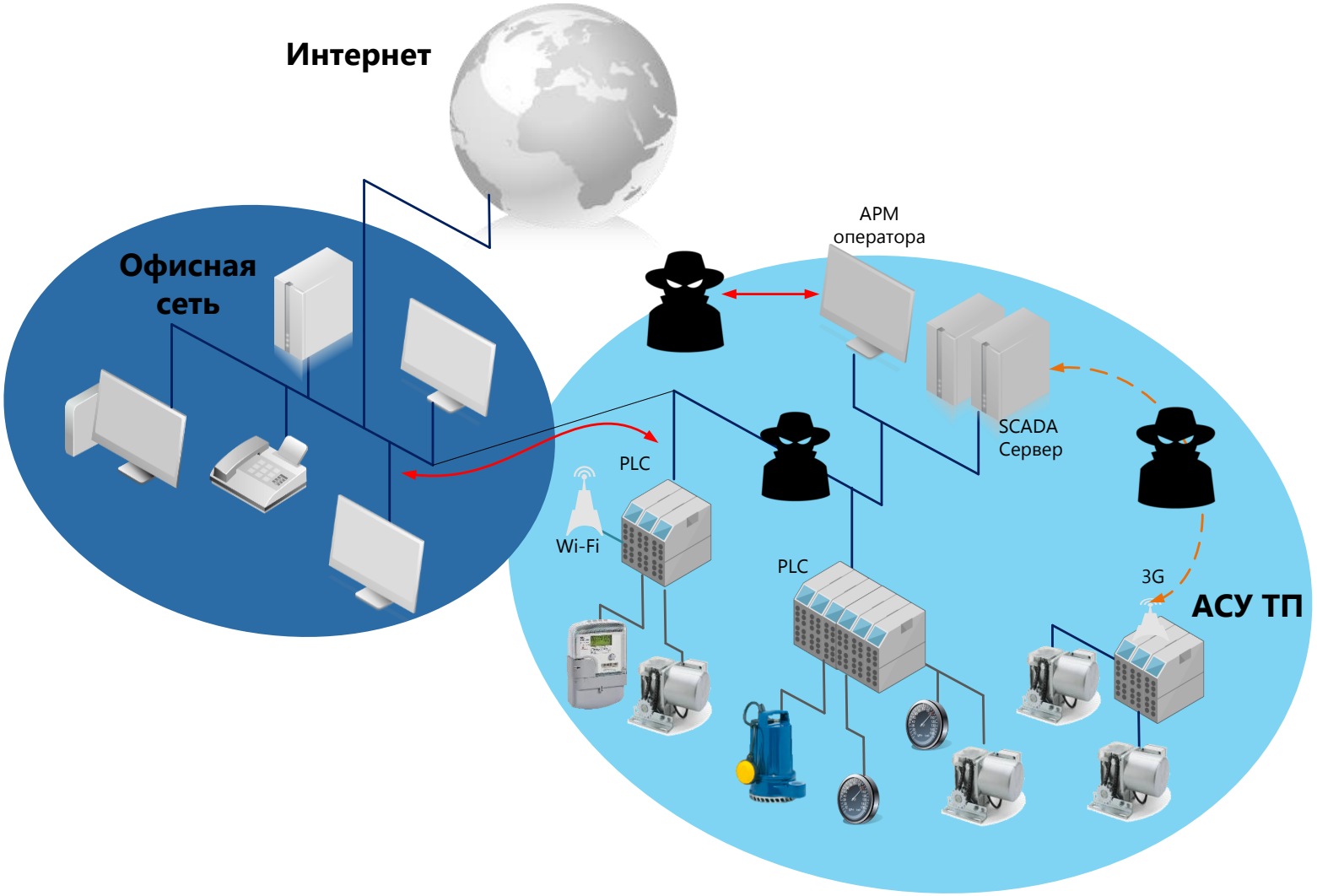
Эволюция АСУ ТП



Ландшафт угроз



Ландшафт угроз



Технический прогресс

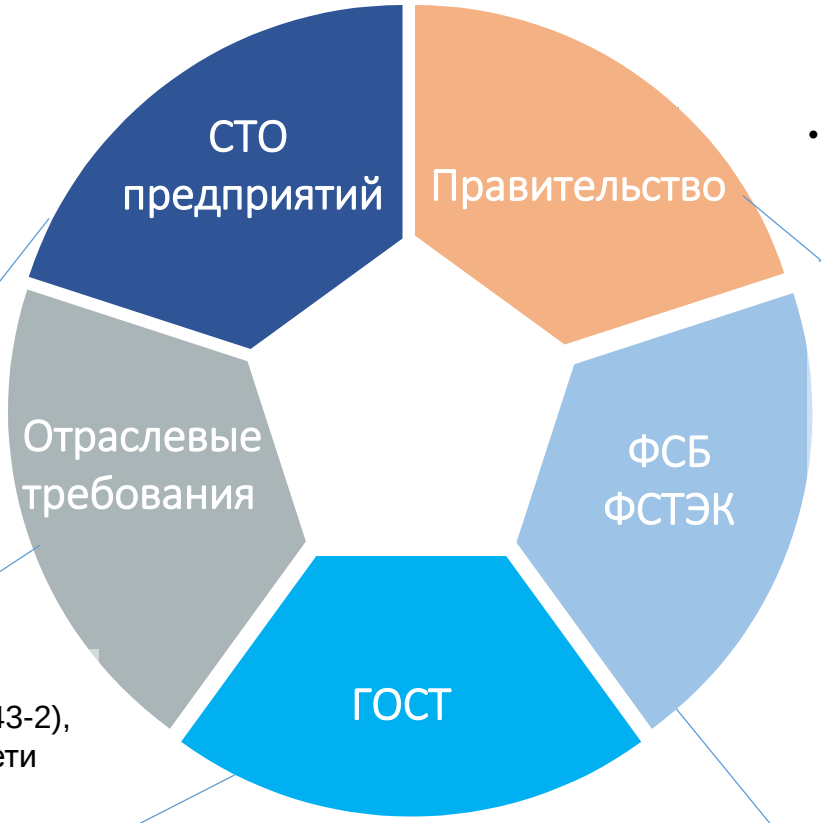
- Массовое внедрение типовых АСУ ТП
- Использование Интернета как транспортной среды
- Интеграция АСУ с ERP и MES
- Отсутствие обновлений АСУ
- Развитие систем дистанционного мониторинга
- Industry 4.0, IIoT, Digital Factory, PLM-системы
- Сервисные модели бизнеса в промышленности

Факторы влияния на вопросы защиты информации в АСУ

- СТО РЖД 02.049-2014 «АСУ ТП ж/д транспорта. Требования к функциональной и информационной безопасности программного обеспечения»
- 05.2016г. Проект требований к ВСЗИ АСУ ТП электросетевого комплекса группы компаний ПАО «Россети»

- ГОСТ «Средства и системы управления железнодорожным тяговым подвижным составом. Требования к программному обеспечению»

- ГОСТ Р 56205 (IEC 62443-1-1), ГОСТ Р МЭК 62443-2 (IEC 62443-2), ГОСТ Р 56498 (IEC 62443-3) Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы.

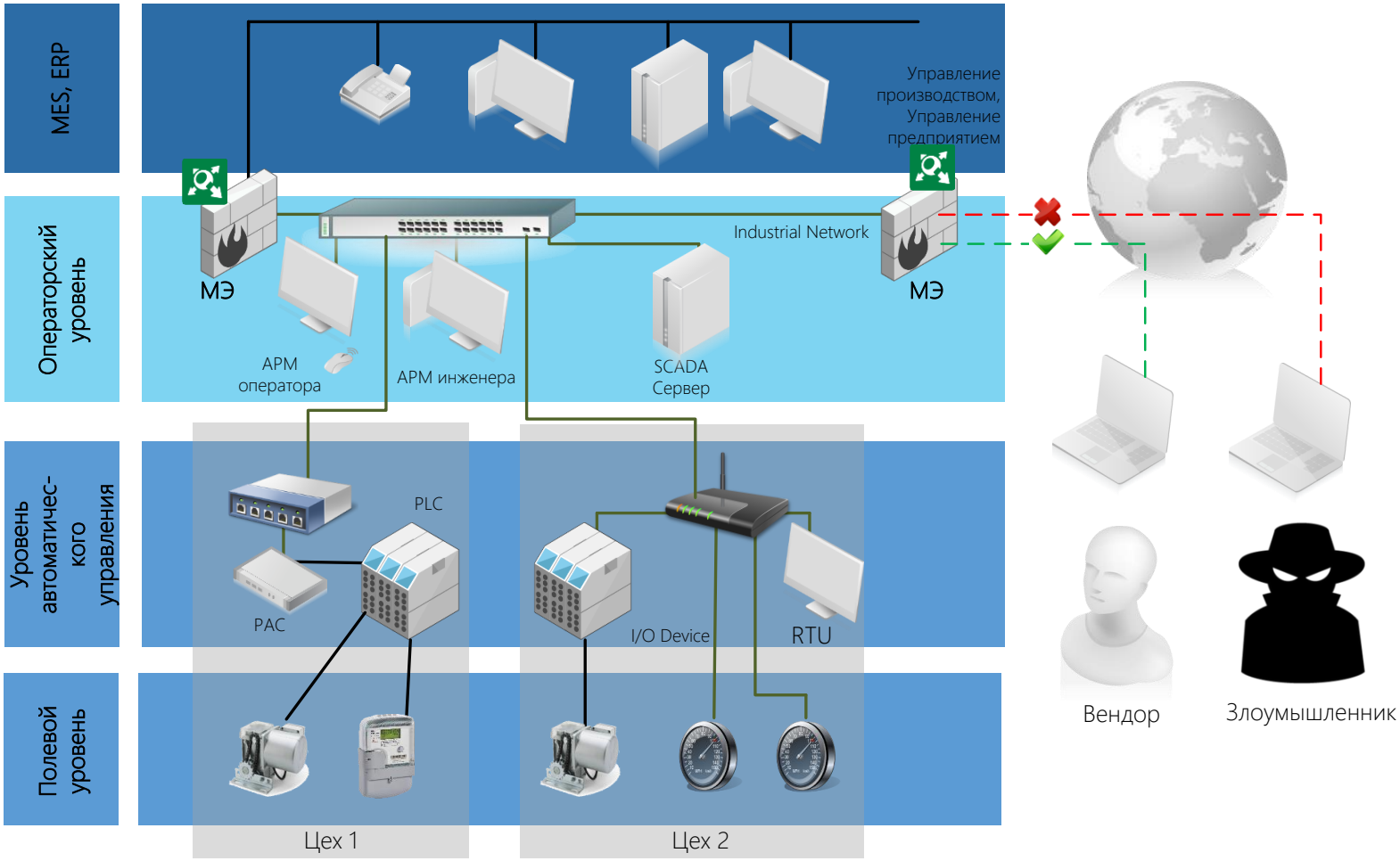


- Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации»
- №256-ФЗ «О безопасности объектов топливно-энергетического комплекса»

- Приказ ФСТЭК России №31 от 14.03.2014 «Об утверждении Требований к обеспечению защиты информации в АСУ ТП»
- "Проект открытых требований к СКЗИ" ФСБ
- «Требования к МЭ» ФСТЭК
- ФСБ: Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. 12.12.14)

Сценарии защиты информации

Защита периметра



- ViPNet Coordinator HW100, HW1000, HW2000
- ViPNet xFirewall

ViPNet Coordinator HW 4

Firewall

- Stateful Packet Inspection
- NAT, Antispoofing
- Application Layer Gateway
- Proxy-server with AV, content filtering

VPN Gateway

- ViPNet Gate
- L2VPN (L2OverIP)
- Traversal NAT

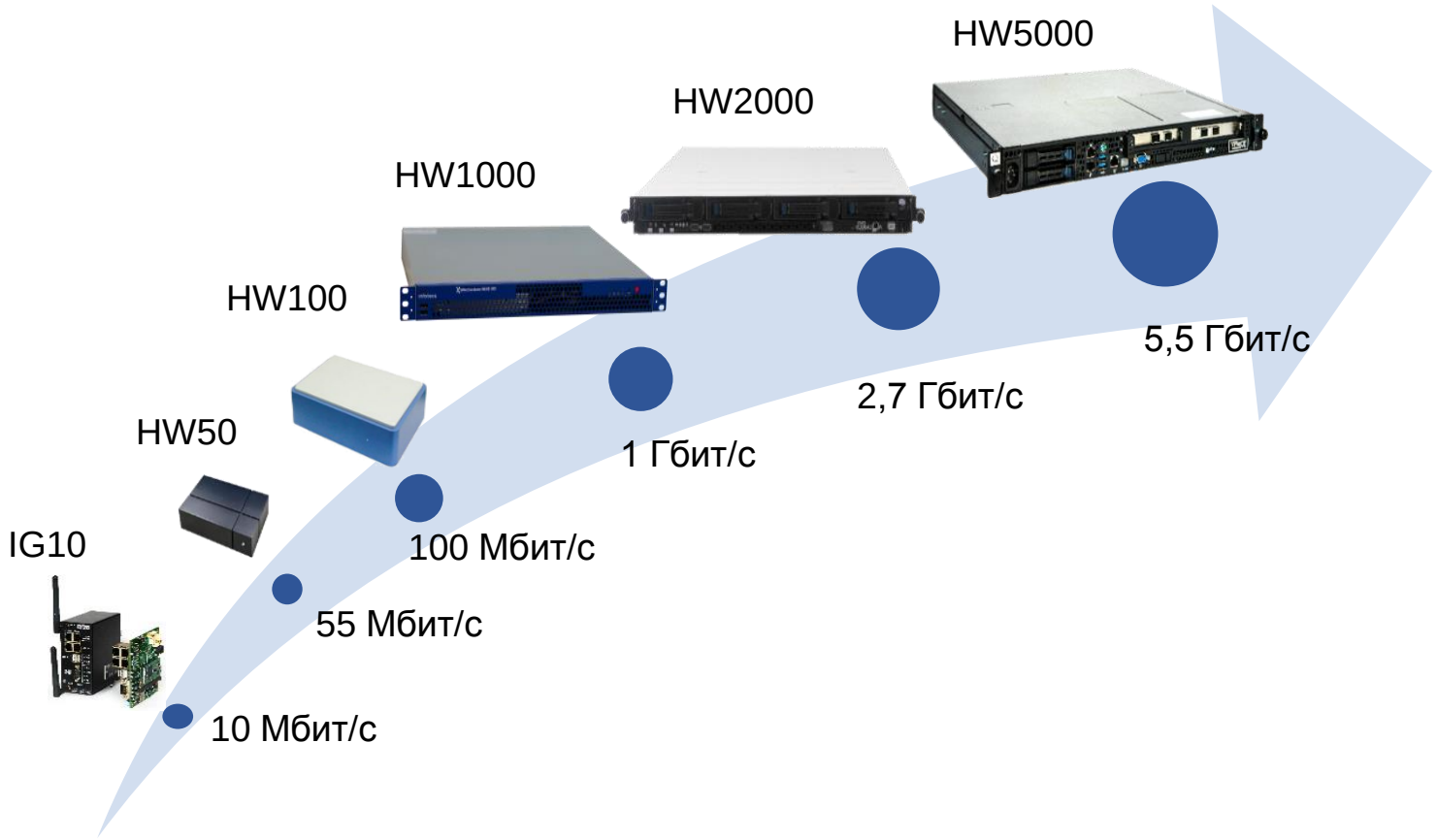
Network services

- DNS,
- NTP-server,
- DHCP-server,
- DHCP-Relay
- VLAN, QoS support

Transport server

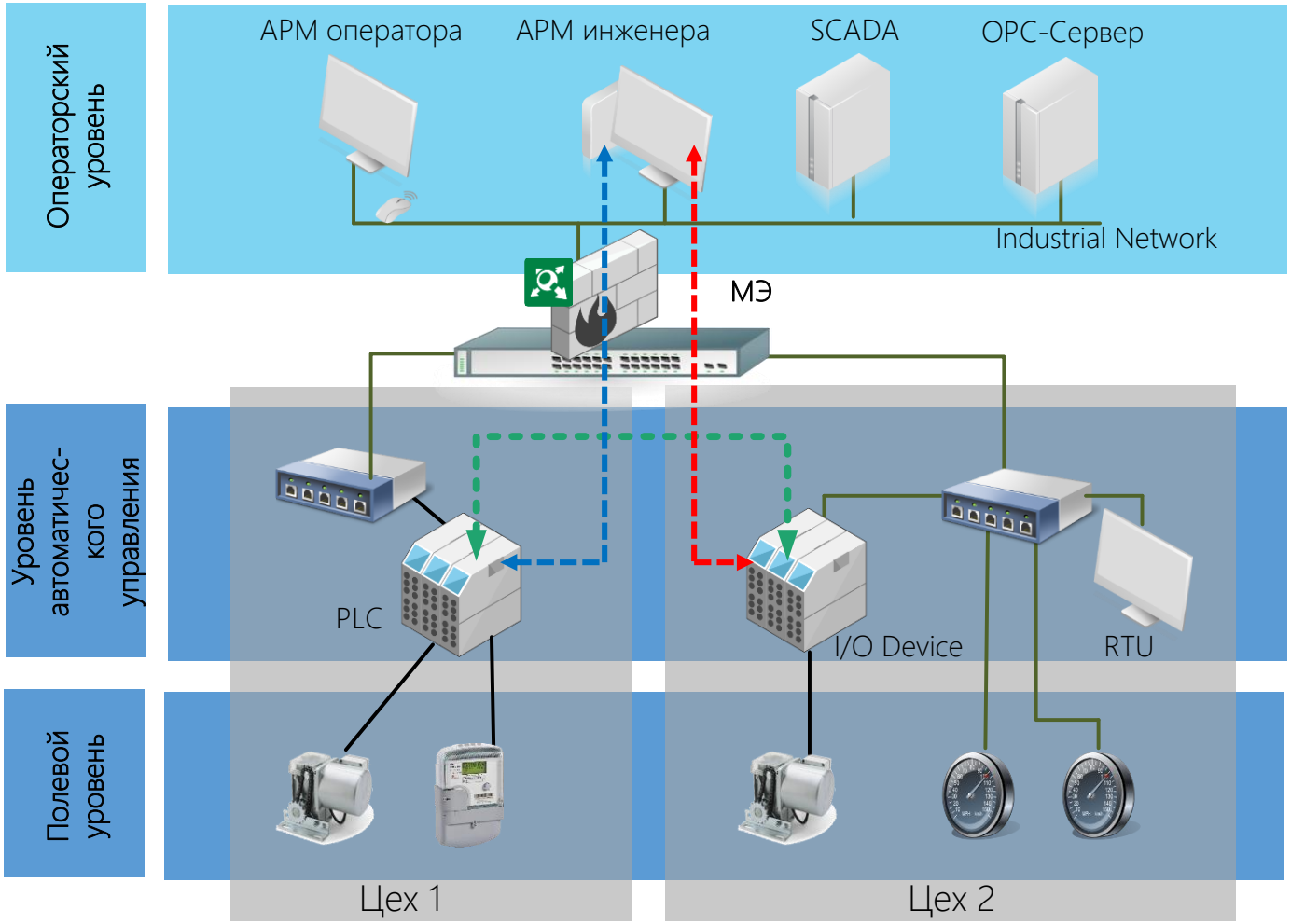
Failover

ViPNet Coordinator HW 4



ViPNet xFirewall

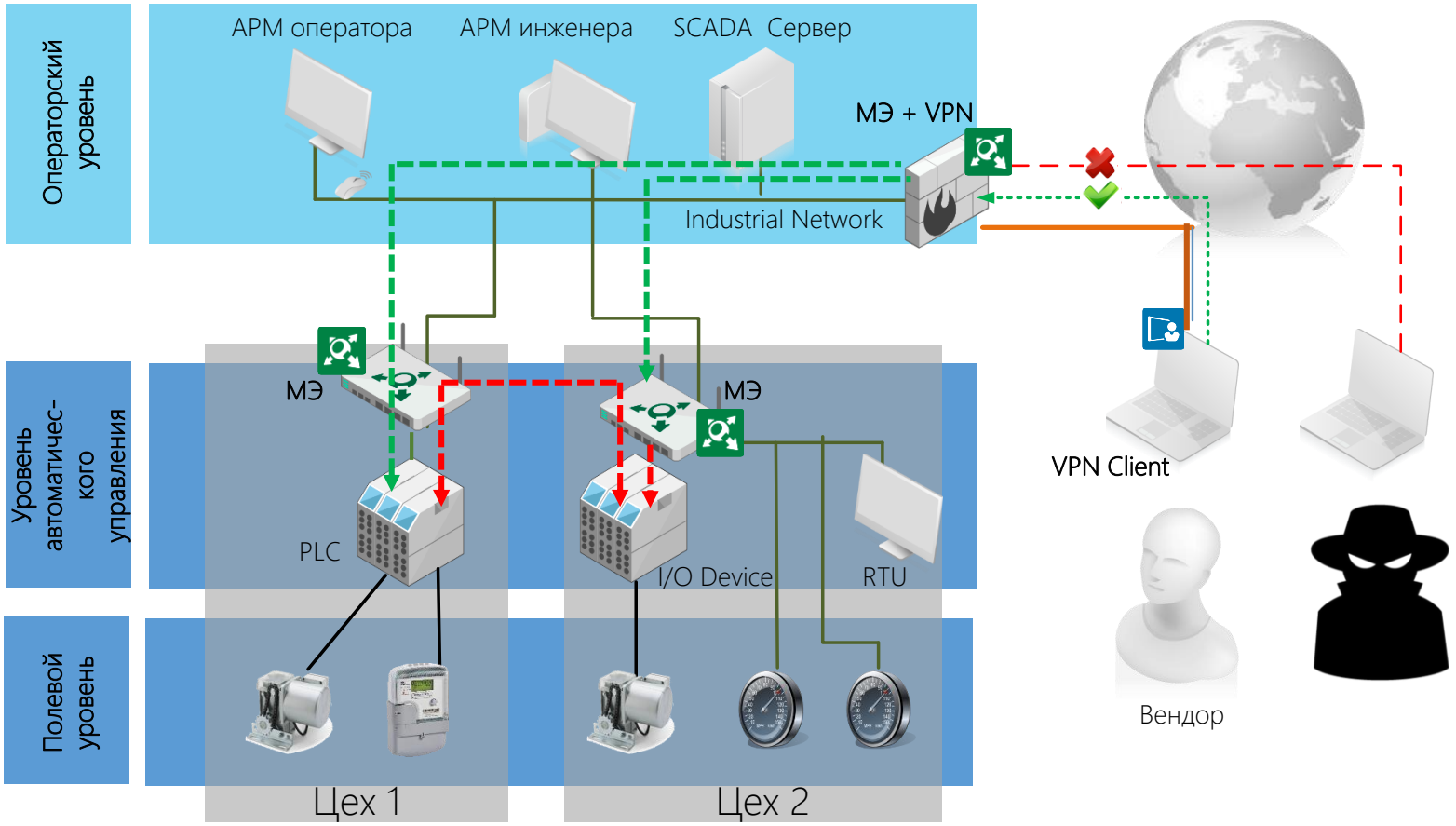
Сегментирование



ViPNet Coordinator HW100, HW1000, HW2000

ViPNet xFirewall

Эшелонирование



ViPNet Coordinator HW

ViPNet xFirewall

ViPNet Client

ViPNet Coordinator IG

Промышленный криптошлюз ViPNet Coordinator IG

- Защищенный канал VPN с поддержкой L2overIP (до 10 Мбит/с)
- Межсетевой экран
- Индустриальное исполнение (-20^0... +60^{0}C, IP30, 10...30 V DC, DIN-рейка)
- Сетевые функции (DNS,DHCP, VLAN)
- Беспроводные интерфейсы (3G, LTE, Wi-Fi)
- Работа в режиме шлюза (Ethernet - RS-232/RS-485) и моста Modbus TCP - Modbus RTU
- Дискретные порты ввода-вывода (GPIO)
- Собственная схемотехника

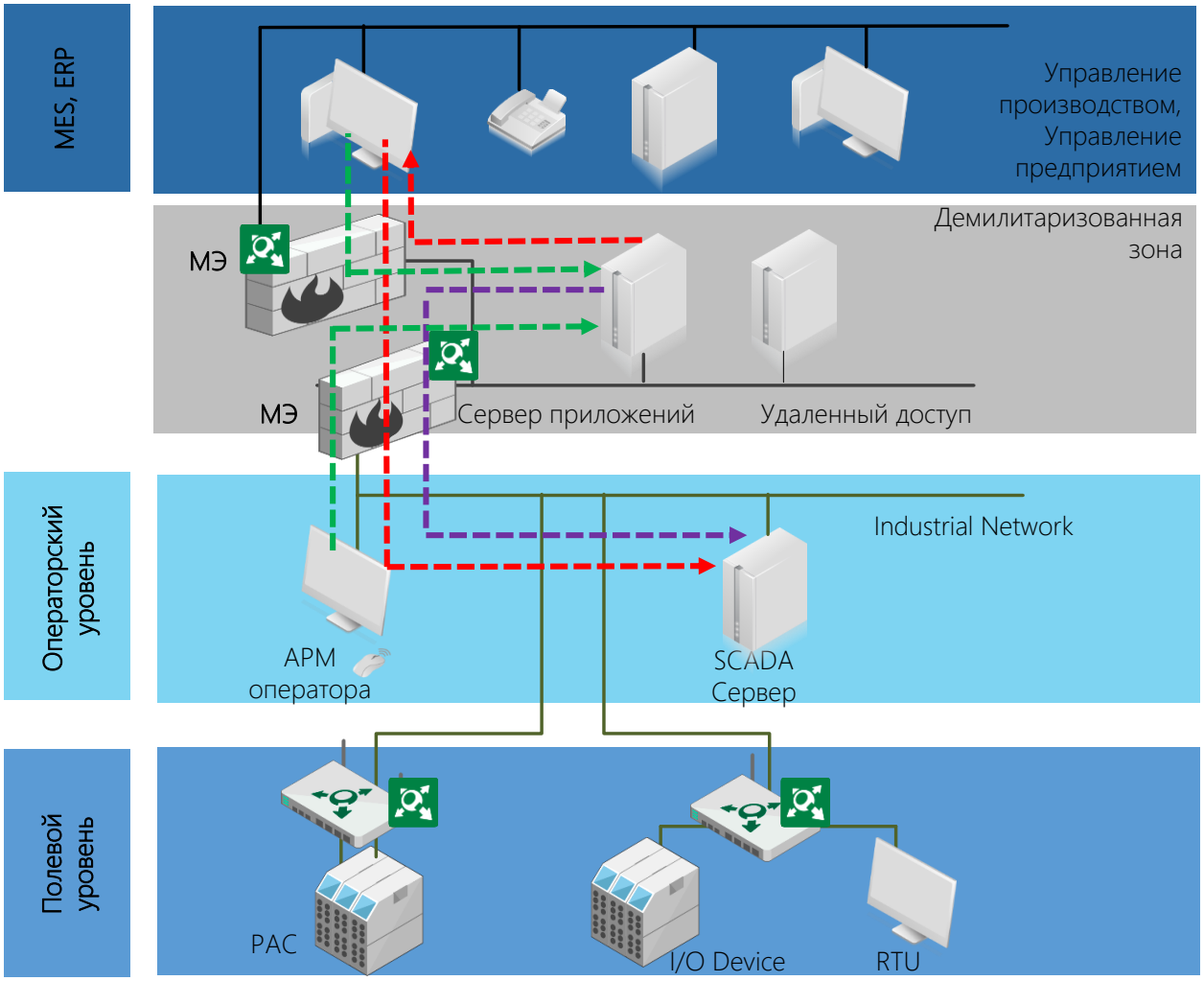
ViPNet Client

infotecs

ViPNet Client

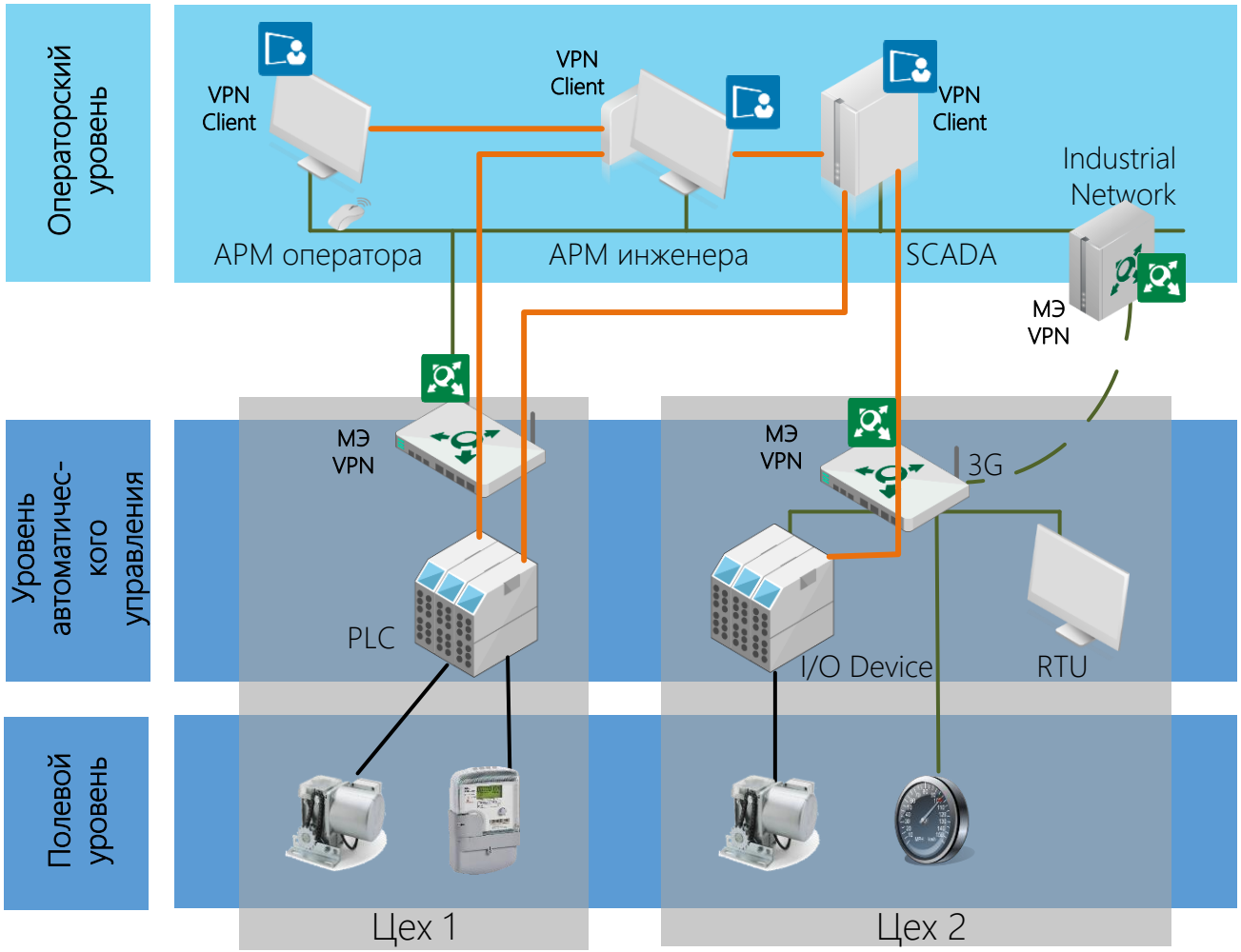
Функционал	VPN
	Персональный сетевой экран
	Конфигурации и политики
	Агент мониторинга
Исполнение	Программный комплекс Windows, Linux, iOS, Android, MacOS, TIZEN
	ViPNet Terminal
	КС1-КС3

Демилитаризованная зона



- ViPNet Coordinator HW
- ViPNet xFirewall
- ViPNet Coordinator IG

VPN и аутентификация

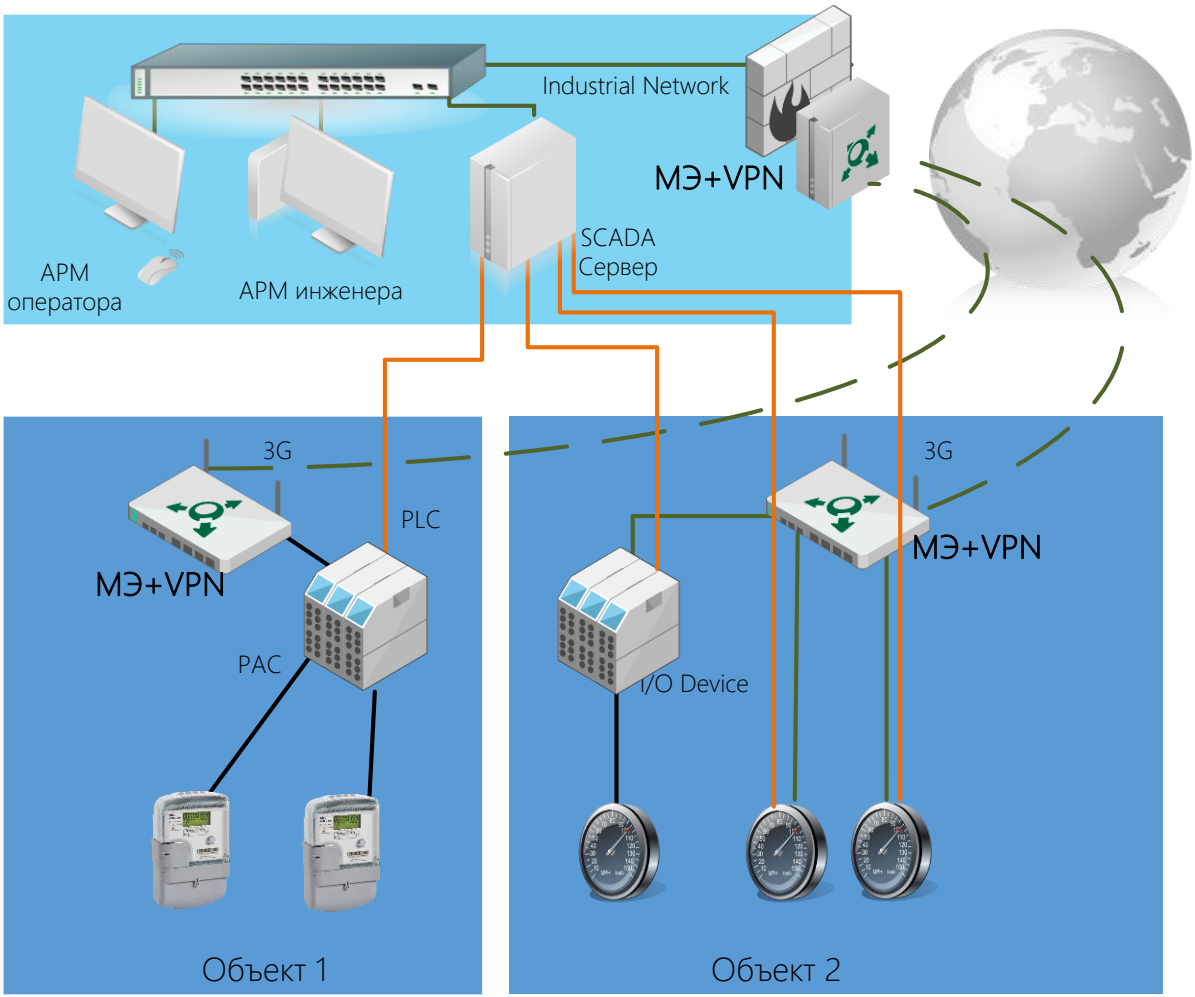


ViPNet Coordinator HW

ViPNet Coordinator IG

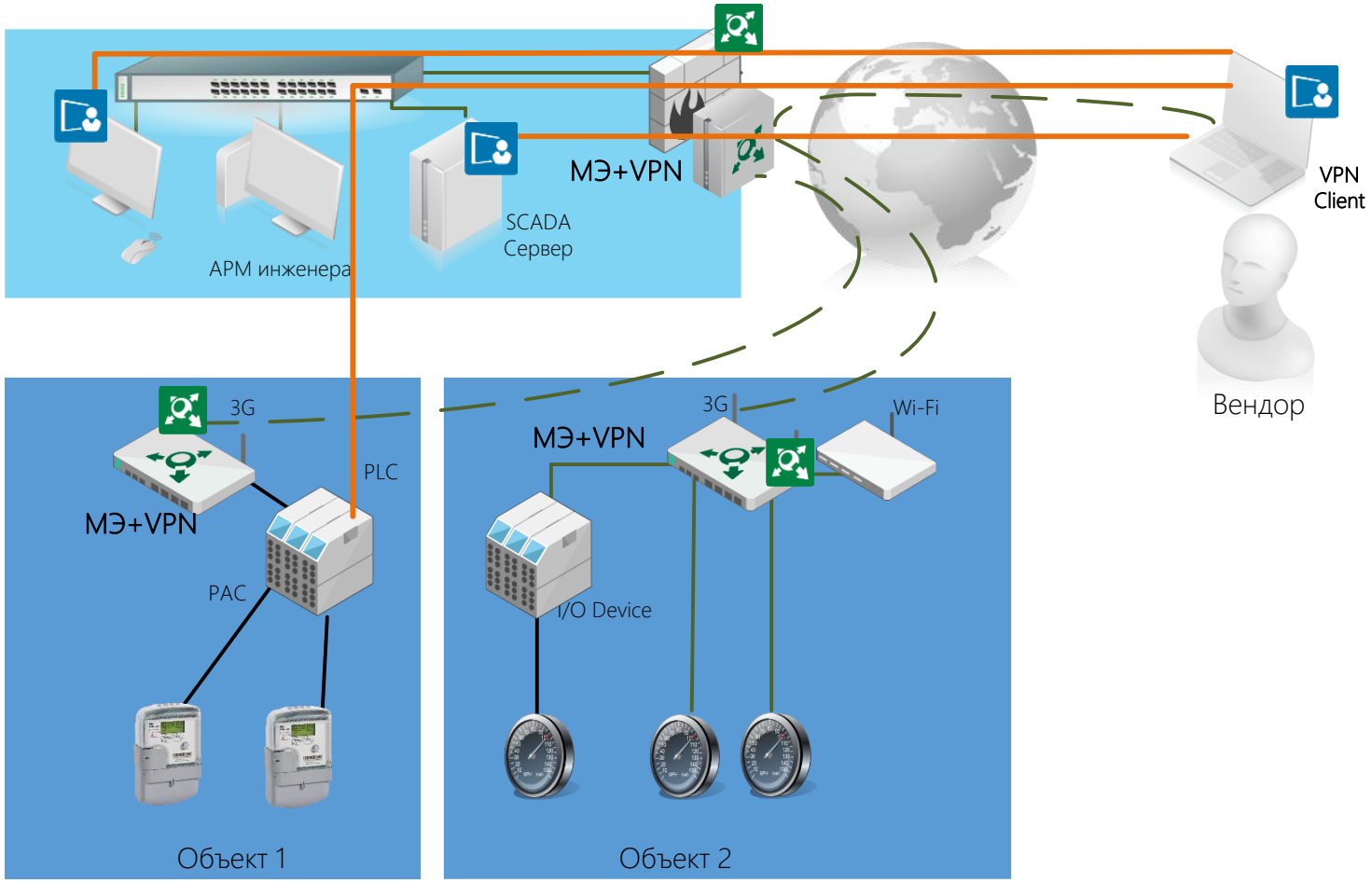
ViPNet Client

Удаленный мониторинг



- ViPNet Coordinator HW
- ViPNet Coordinator IG
- ViPNet xFirewall

Удаленное управление и конфигурирование



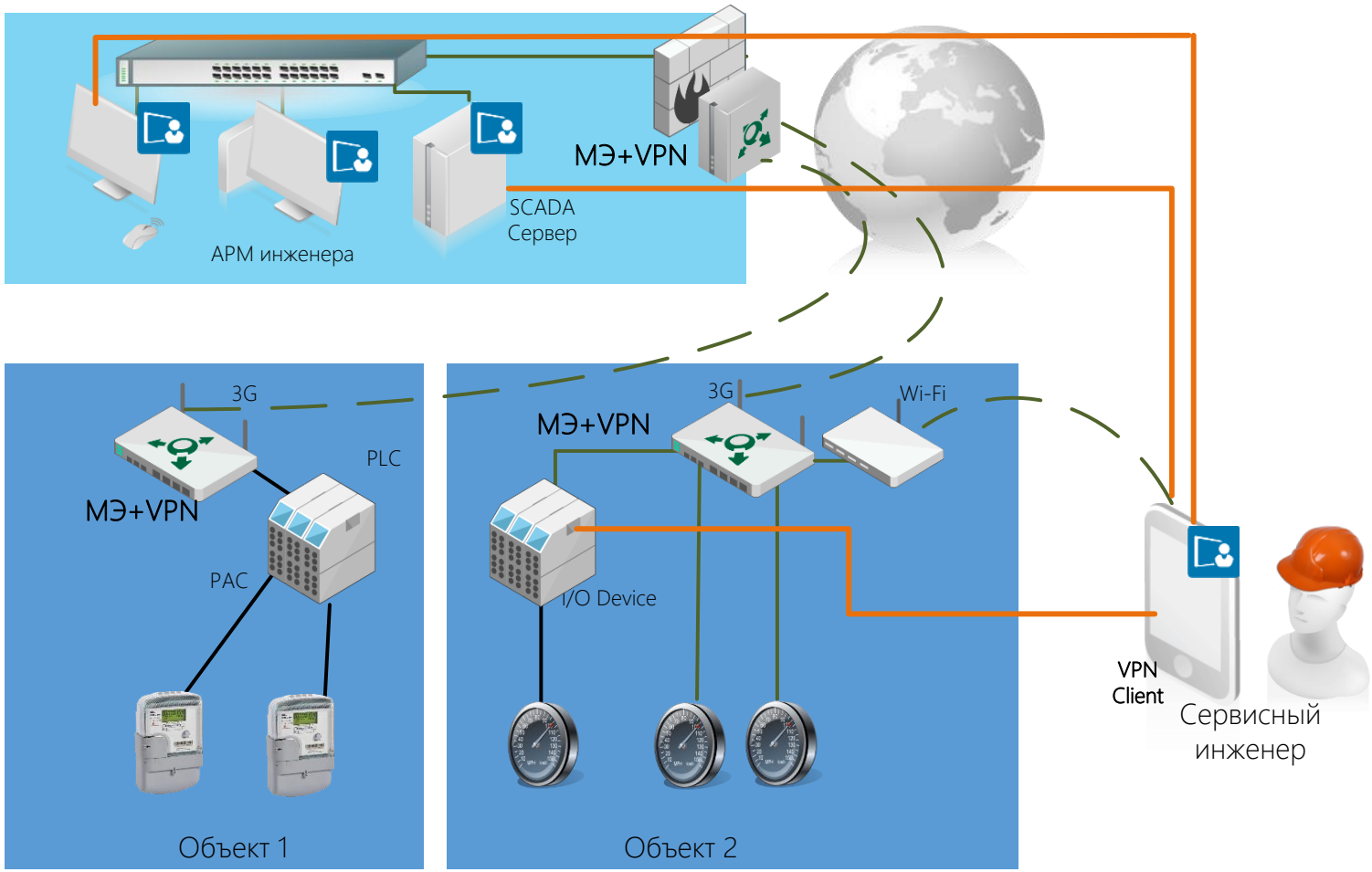
ViPNet Coordinator HW

ViPNet xFirewall

ViPNet Client

ViPNet Coordinator IG

Телесервис



ViPNet Coordinator HW

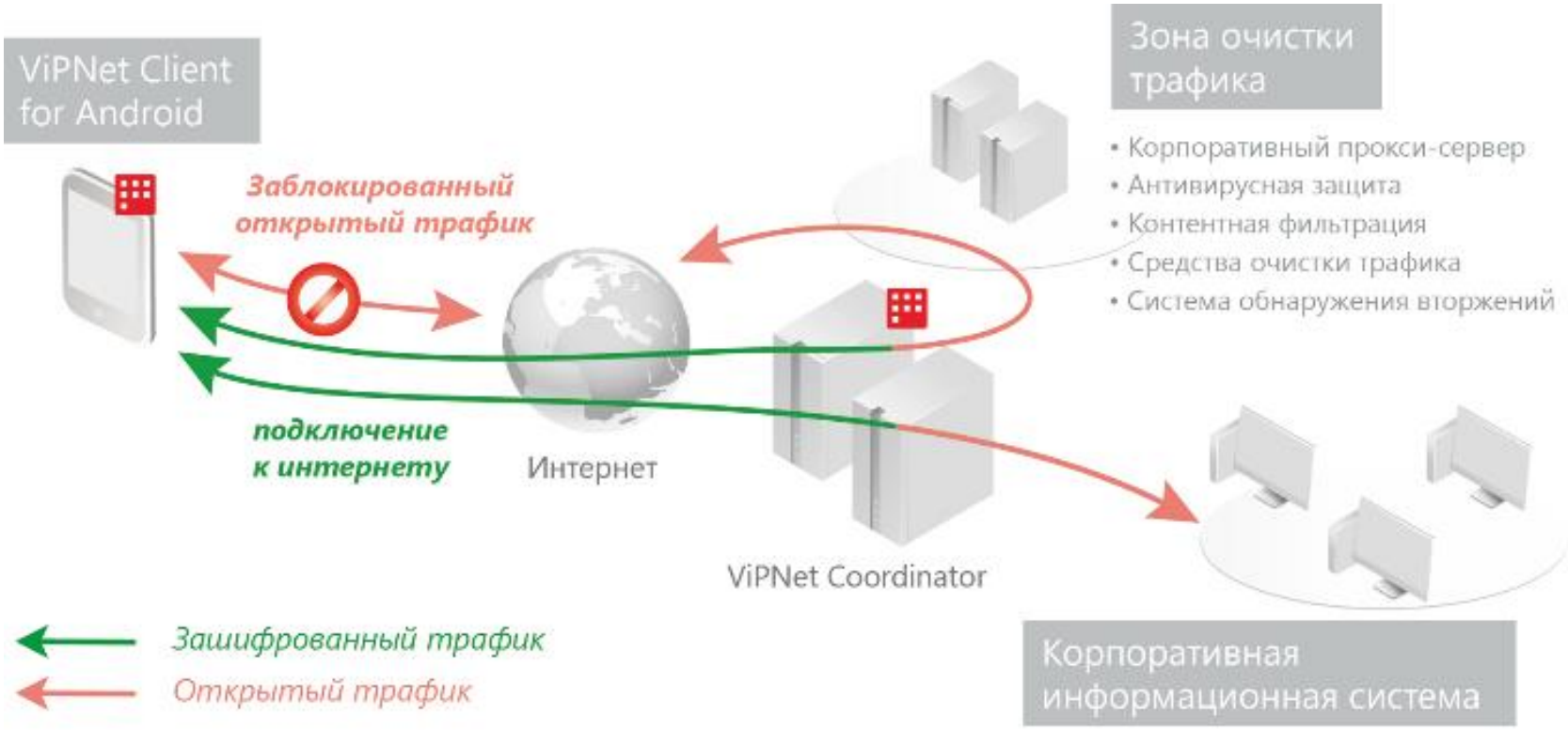
ViPNet xFirewall

ViPNet Client

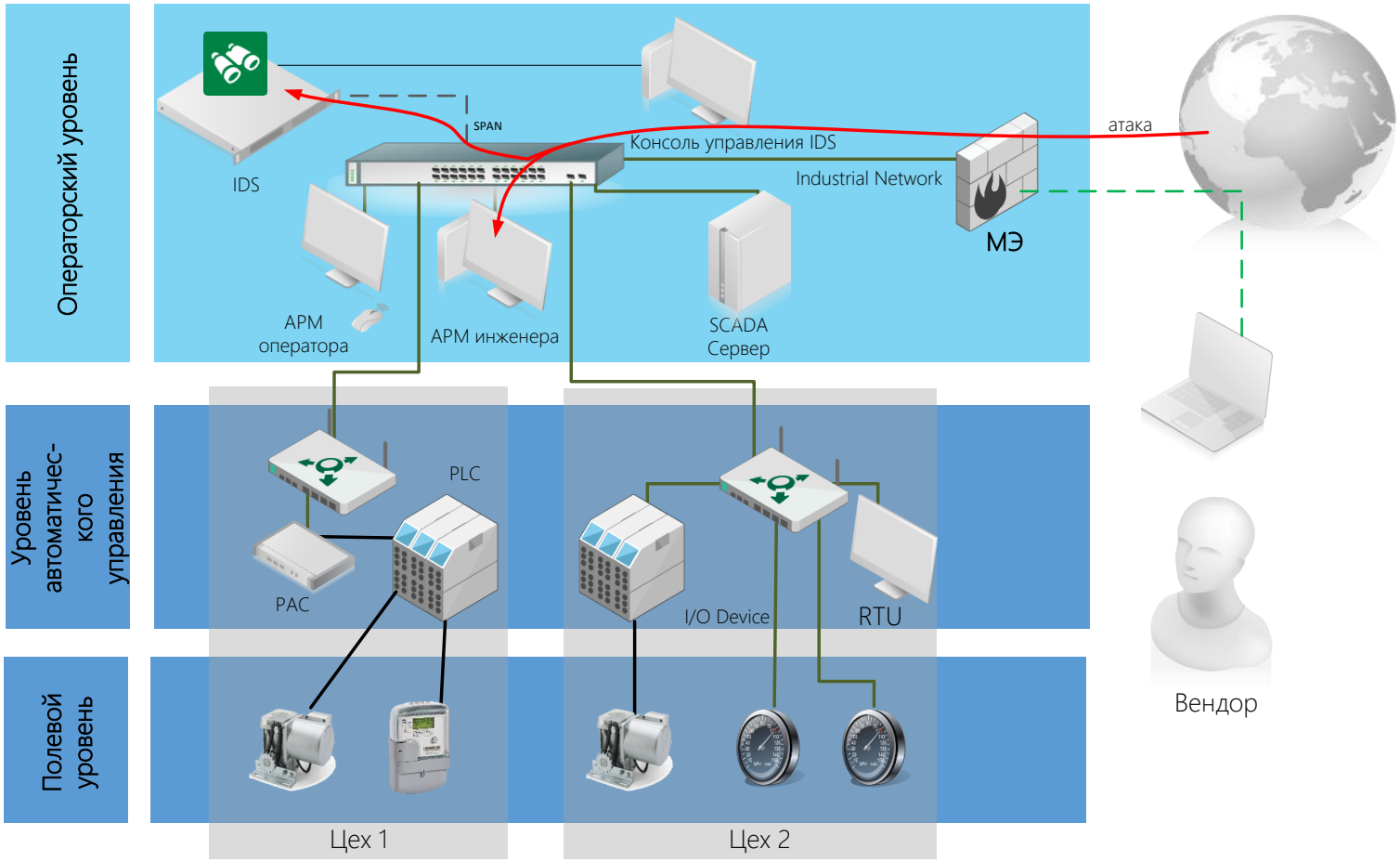
ViPNet Coordinator IG

Мобильная версия ViPNet Client

Схема защиты



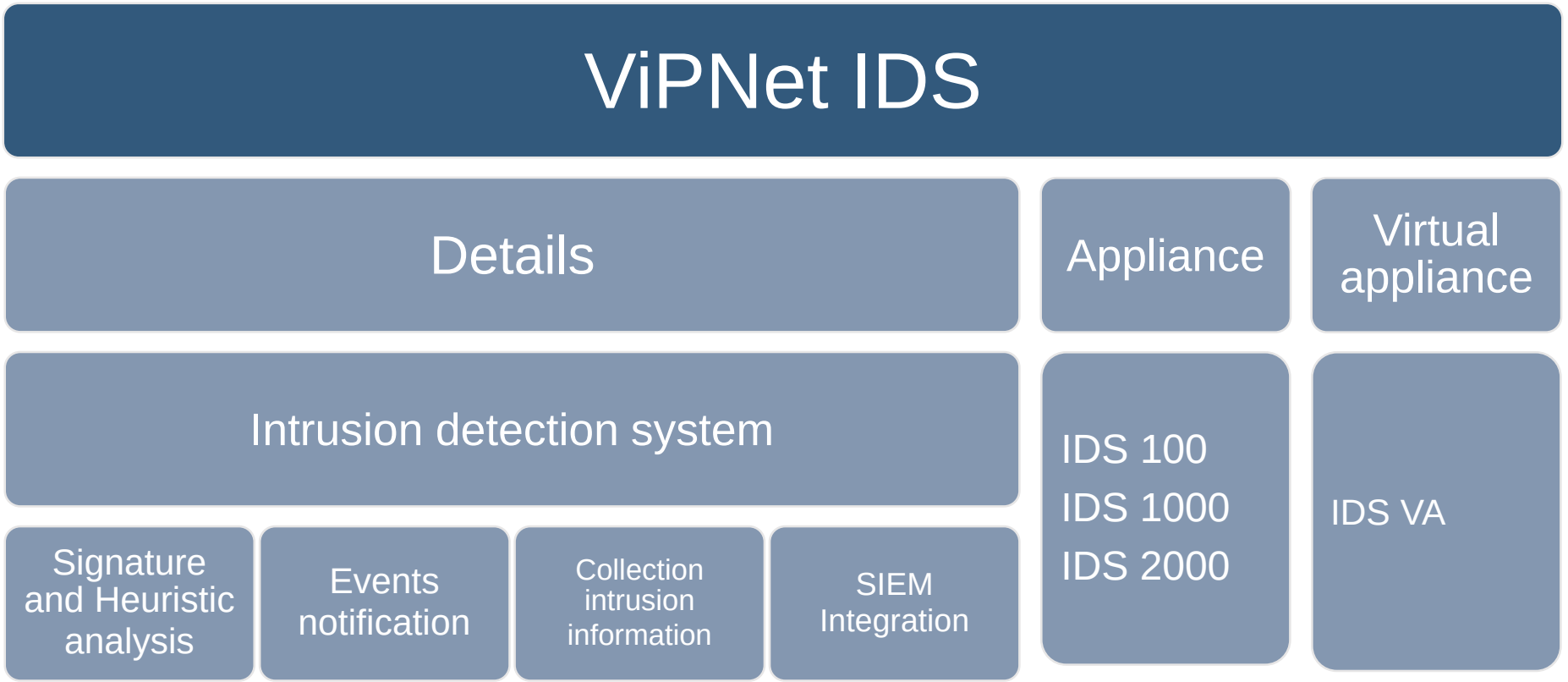
Мониторинг и система обнаружения вторжений



ViPNet IDS

ViPNet IDS

Система обнаружения атак



ViPNet IDS

Поставщики сигнатур атак

Cisco	• VRT, Talos
Emerging Threats	• Emerging Threats Pro
StoneSoft	~~• StoneSoft~~
Infotecs	• AM Rules

ViPNet IDS

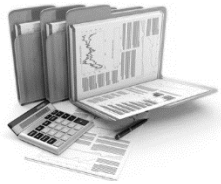
Сравнение поставщиков сигнатур атак

Cisco	ET	ИнфоТеКС
32665	30034	24866
250-300 новых сигнатур	300-400 новых сигнатур	300-400 новых сигнатур
ZeroDay сигнатуры	ZeroDay сигнатуры	ZeroDay сигнатуры
Страна происхождения - США	Страна происхождения - США	Страна происхождения Россия

Сквозная безопасность

ERP, MES

Системы управления предприятием
Системы планировани производства



ViPNet Network Security

Операторский уровень АСУ ТП

SCADA
АРМ оператора
Центры управления и мониторинга

ViPNet Coordinator HW,
ViPNet Coordinator IG
ViPNet Client (desktop, laptop, mobile)
ViPNet xFirewall
ViPNet IDS

Полевой уровень АСУ ТП

ПЛК
Исполнительная среда

ViPNet Coordinator IG


Спасибо!
Marina.Sorokina@infotecs.ru
Марина Сорокина